ESCOLA SUPERIOR DE ENFERMAGEM DE COIMBRA

VERSÃO	MOTIVO DA REVISÃO	ELABORADO POR	APROVADO POR	DATA APROVAÇÃO
0.1	Criação e redação preliminar	Serviço de Informática	N/A	N/A
1.0	Redação final	Serviço de Informática	Presidente da Escola	08/02/2023

Elaboração	Verificação	Aprovação
SERVIÇO DE INFORMÁTICA	Dulce Silva	
Data: 8 . 2 . 2023	Data: 8 . 2 . 2023	Data: 8 . 2 . 23

Presidência	**ESCOLA SUPERIOR DE ENFERMAGEM DE COIMBRA** **DESPACHO N.º 17 – PRESIDENTE**	Data: 08/02/2023

Nos termos do número 1 do artigo 8º e da alínea m) do número 1 do artigo 49º dos Estatutos da Escola Superior de Enfermagem de Coimbra, aprovados por Despacho normativo n.º 50/2008 do Ministro da Ciência, Tecnologia e Ensino Superior, publicados em Diário da República, 2.ª série, N.º 185, de 24 de setembro de 2008, aprovo a Política Segurança da Informação e Cibersegurança da ESEnfC - Versão 1.0.

O Presidente

Prof. Doutor António Fernando Salgueiro Amaral

Escola Superior de
Enfermagem de Coimbra

Política Segurança da Informação e Cibersegurança

Versão 1.0

Índice

1. OBJETIVO DA POLÍTICA

A Escola Superior de Enfermagem de Coimbra (ESEnfC) considera que uma política de informação clara e transparente é essencial para a prossecução da sua missão, sendo um ativo estratégico de considerável valor. A segurança de todo o processo de conceção à utilização da informação produzida é vital para a imagem pública da Escola e para que esta possa servir todos os interessados de forma fiável e como ferramenta essencial à gestão.

Assim, entendemos como fundamental a definição e aplicação de uma política que defina os seus compromissos para a proteção dessa informação, tendo designado um **Responsável pela Segurança** que assegure a gestão da segurança da informação.

O **Responsável de Segurança** deve garantir que esta política se mantém adequada para os objetivos atinentes à segurança da informação e que esteja em condições de sustentar o **Plano de Segurança da ESEnfC**.

A/O Presidente da **ESEnfC**, no âmbito das suas competências, compromete-se a disponibilizar os necessários recursos e suporte, bem como levará a cabo a missão de garantir a melhoria contínua de tais compromissos e respetivas métricas de eficácia, por forma a assegurar a execução dos requisitos e expetativas das partes interessadas identificadas no **Plano de Segurança da ESEnfC**.

2. ÂMBITO DE PROTEÇÃO PARA A SEGURANÇA DA INFORMAÇÃO

O âmbito de proteção, onde se aplica esta política, está descrito no **Plano de Segurança da ESEnfC**, que o apresenta como sendo a proteção de toda a informação captada, processada, armazenada e transferida, assim como os ativos/recursos que são usados para execução dos serviços essenciais.

3. PARTES INTERESSADAS

Entende-se como partes interessadas, todas as pessoas singulares, instituições públicas ou privadas que interagem com o âmbito de proteção para a Segurança da Informação e Cibersegurança, identificando requisitos ou expectativas de Segurança da Informação e/ou Cibersegurança.

Constituem **partes interessadas internas** os Órgãos de Governo, o Corpo Discente e Corpo Docente e os Colaboradores contratados da instituição.

Constituem **partes interessadas externas**, para a presente versão do plano, as seguintes instituições e organismos:

- Administração Pública Central de tutela ao Ensino Superior;
- Direção Geral de Estatísticas da Educação e Ciência;
- Direção Geral do Ensino Superior
- Direção Geral da Administração e do Emprego Público;
- Direção Geral da Educação

- Fundação para a Ciência e Tecnologia;
- Entidade de Serviços Partilhados da Administração Pública, I. P.;
- A3ES - Agência de Avaliação e Acreditação do Ensino Superior;
- Entidades reguladoras – Centro Nacional de Cibersegurança; Comissão Nacional de Proteção de Dados;
- Instituições de Ensino Superior parceiras;
- Instituições que recebem estágios nos seus vários moldes;
- Docentes convidados;
- Prestadores de Serviços/fornecedores.

4. COMPROMISSOS PARA A SEGURANÇA DA INFORMAÇÃO

A presente Política define os compromissos assumidos pela **ESEnfC,** no âmbito de proteção para a segurança da informação, que consistem nas seguintes garantias:

- **Confidencialidade** – Assegurar que apenas os utilizadores formalmente autorizados têm acesso à informação;
- **Privacidade** – Assegurar que os dados pessoais dos respetivos titulares, classificados como informação confidencial, apenas são recolhidos, tratados e armazenados de acordo com fundamento legal válido nos termos dos princípios do quadro legal vigente;
- **Integridade** – Assegurar a proteção da informação contra a modificação e/ou destruição não autorizada, salvaguardando a respetiva veracidade e autenticidade;
- **Disponibilidade** – Assegurar que o acesso à informação é realizado sempre que necessário para a realização de uma atividade, preservando a confidencialidade, privacidade e integridade;
- **Não Repúdio** – Assegurar que todos os utilizadores autorizados quando na condição de emissores de informação ou quando partilham dados pessoais com destinatários autorizados, serão sempre identificados física e digitalmente com valor probatório legal;

5. PLANO DE SEGURANÇA

O Plano de Segurança da **ESEnfC** tem como missão a definição, implementação, manutenção e melhoria contínua de um conjunto de políticas, regras e práticas, medidas e controlos de segurança, ações de monitorização e auditoria que permitam garantir a execução dos compromissos assumidos pela ESEnfC para a gestão da Segurança da Informação e da Cibersegurança.

Para atingir, com eficácia, os compromissos e objetivos assumidos na presente política serão adotados os seguintes mecanismos de operacionalização:

- Definição, aprovação e divulgação de políticas temáticas complementares para a gestão da Segurança da Informação;
- Promoção de ações de sensibilização, formação e treino dos colaboradores e comunidade académica;
- Análise e gestão dos riscos identificados, incluindo o(s) respetivo(s) plano(s) de tratamento do risco e o respetivo risco residual;
- Identificação e operacionalização de controlos de segurança para tratamento do risco;

- Gestão dos incidentes de segurança de informação, e respetivas respostas, para garantia da continuidade de serviços nas atividades definidas no âmbito de proteção;
- Realização de auditorias internas para identificação de oportunidades de melhoria;
- Revisão do Plano de Segurança e respetivas métricas de eficácia.

6. GESTÃO DO RISCO

Por se considerar uma ferramenta imprescindível no cumprimento dos objetivos do **Plano de Segurança da ESEnfC,** serão feitas, periodicamente, análises de risco com o objetivo de serem adotadas as medidas de tratamento adequadas e proporcionais aos níveis do risco identificados.

Os controlos de segurança a implementar serão selecionados em função dos resultados dessa análise, com objetivo de assegurar a redução do risco, com eficácia, e a minimização do risco residual.

7. INTEGRAÇÃO COM A GESTÃO DA PRIVACIDADE DE DADOS PESSOAIS

Através da definição da garantia de privacidade como um dos compromissos da segurança da informação, a **ESEnfC** executa a implementação integrada de controlos de segurança que asseguram as medidas de tratamento do risco adequadas para cumprimento dos requisitos do Regulamento Geral sobre a Proteção de Dados, e legislação conexa.

8. CIBERSEGURANÇA

A informação crítica para os serviços essenciais, assim como os dados pessoais utilizados pelos processos internos da **ESEnfC**, em função da definição do âmbito de proteção, serão protegidos adequadamente contra os ataques e ameaças externos ou internos que sejam realizados através de mecanismos ou métodos que coloquem em causa a Cibersegurança da **ESEnfC** e de todos quantos com a mesma interagem.

Para este efeito, entende-se como Cibersegurança a garantia de que os compromissos de segurança desta política são assegurados, mesmo havendo lugar a possíveis exposições ao Ciberespaço e, como consequência, serem alvo de Ciberataques.

A ESEnfC cumprirá os requisitos e práticas determinados pelo quadro legal que constitui o ***Regime Jurídico da Segurança do Ciberespaço,*** e procederá à adoção de boas práticas, medidas e controlos de segurança adequados, constantes no **QNRCS** - ***Quadro Nacional de Referência para a Cibersegurança***, na norma ISO/IEC 27001 e ISO/IEC 27002, nas recomendações da *European Union Agency for Cybersecurity* (ENISA), bem como implementará os procedimentos de gestão de incidentes necessários para identificar e tratar ataques ou ameaças.

Complementarmente, implementará medidas de prevenção e proteção adequadas e proporcionais para assegurar o cumprimento das obrigações assumidas na presente política.

9. GESTÃO DE INCIDENTES

Um incidente de segurança ocorre quando um dos compromissos de segurança, incluídos na presente política, é violado, ou seja, não é possível ser mantido e demonstrado.

A **ESEnfC** compromete-se a implementar um procedimento de gestão de incidentes, supervisionado pelo Responsável de Segurança, tendo como objetivo a contenção do possível impacto de um ataque interno ou externo, e a retoma do funcionamento dos seus serviços essenciais o mais rapidamente possível.

Ciente da sua responsabilidade para com as partes interessadas, este procedimento inclui atividades de comunicação que permitem informar adequadamente do estado de evolução e tratamento de qualquer incidente de segurança.

Neste contexto, destaca-se a integração do procedimento de notificação de incidentes de Cibersegurança à entidade nacional designada, Centro Nacional de Cibersegurança.

10. FUNÇÕES E RESPONSABILIDADES

Os intervenientes com funções e responsabilidades em relação á gestão e aplicação desta política são os seguintes:

1. Liderança – Presidente

O Presidente da **ESEnfC** assegura que a presente política e os objetivos de segurança estão estabelecidos e são adequados para com a orientação estratégica da **ESEnfC**, assim como a integração dos requisitos de segurança da informação nos processos organizativos, bem como os recursos necessários para gestão eficaz do Plano de Segurança.

A/O Presidente da **ESEnfC** aprova e delibera, no âmbito das duas competências, as medidas necessárias para a implementação com eficácia do **Plano de Segurança da ESEnfC**. Caso considere adequado a/o Presidente apresenta para aprovação do Conselho de Gestão, medidas que sejam da estrita competência desse Órgão.

2. Responsável de Segurança

O Responsável de Segurança é um recurso da ESEnfC, nomeado pela/o Presidente.

Tem a seu cargo as seguintes responsabilidades:

- Aprovar e melhorar continuamente o Plano de Segurança;
- Acompanhar a implementação e operacionalização do Plano de Segurança;
- Supervisionar e aprovar o inventário de ativos essenciais;
- Supervisionar a realização periódica da análise do risco e a definição do plano de tratamento do risco, apresentado os respetivos resultados à Direção da ESEnfC;
- Identificar o risco residual decorrente das medidas de tratamento do risco e propor a respetiva aceitação pela Direção da ESEnfC;
- Supervisionar a execução e eficácia do procedimento de gestão de incidentes e a recuperação do modo normal de utilização dos serviços essências, assim como das respetivas lições aprendidas;

- Assegurar a conformidade para com a legislação e regulamentação aplicável, incluindo o Regime Jurídico da Segurança do Ciberespaço e o QNRCS;
- Promover a elaboração de planos de formação/sensibilização/consciencialização relativos à segurança da informação e Cibersegurança para as partes interessadas internas da instituição;
- Gerir a execução de auditorias internas de Segurança da Informação e Cibersegurança;
- Aprovação do relatório anual para o CNCS, respetiva validação pela Direção da ESEnfC e envio formal ao CNCS.

3. *Pontos de Contacto Permanente*

O Presidente da **ESEnfC** é responsável pela designação de, pelo menos, um Ponto de Contacto Permanente. A **ESEnfC** deverá assegurar que os recursos designados e comunicados ao CNCS, são em número suficiente para assegurar as responsabilidades abaixo indicadas.

Estes recursos assumem as seguintes funções:

- Assegurar os fluxos de informação de nível operacional e técnico com o CNCS, em conformidade para com o determinado pelo ponto 1 do Artigo 4º do DL 65/2021;
- Disponibilidade para a execução destas responsabilidades num regime de 24/24h e 7 dias por semana;
- Implementar e operacionalizar as medidas de segurança decorrentes das decisões de tratamento do risco para a Segurança da Informação e Cibersegurança;
- Proceder à classificação de incidentes (relevantes ou substanciais)
- Proceder à execução de tarefas relacionadas com a implementação e operacionalização das medidas e controlos de segurança
- Executar procedimentos de resposta a incidentes de segurança e os respetivos relatórios de acompanhamento e resolução para o CNCS;
- Prestar apoio a todos os colaboradores da ESEnfC em matérias de segurança da informação e Cibersegurança;
- Criação do relatório anual para o CNCS, respetiva validação pela Direção da ESEnfC e envio formal ao CNCS;
- Seguindo as instruções do Responsável de Segurança, promover a articulação de informação com outras entidades para melhorar a eficácia da resposta a incidentes de segurança com impacto nas atividades da ESEnfC, nomeadamente com o CNCS.

4. *Comunidade Educativa e Colaboradores*

A Comunidade Educativa e Colaboradores da instituição serão incluídos em planos de formação e ações de sensibilização diferenciadas condizentes com as competências decorrentes dos estatutos da ESEnfC e grau de exposição ao Ciberespaço, em conformidade com os objetivos e obrigações previstas na presente política.

Após a divulgação e publicação desta Política, fica a Colaboradores obrigados a:

- Frequentar as ações de formação incluídas no plano de formação em vigor, seja aquando da sua integração na **ESEnfC**, aquando de mudança de funções ou de acordo com a definição de periodicidade de repetição de cada ação de formação;
- Proteger os ativos de informação a seu cargo;

- Colaborar na gestão do respetivo risco dos recursos atribuídos;
- Assegurar que os recursos que são atribuídos são apenas usados para fins profissionais;
- Participar qualquer evento que possa colocar em causa a segurança da informação;
- Cumprir e fazer cumprir a presente política.

Após a divulgação e publicação desta Política, fica a Comunidade Educativa obrigada a:

- Proteger os ativos da instituição aos quais tenham acesso autorizado;
- Fazer um uso seguro seguindo as recomendações de segurança de credenciais de acesso a sistemas e equipamentos aos quais a **ESEnfC** concede acesso autorizado;
- Tomar conhecimento e cumprir com qualquer informação comunicada pela **ESEnfC** no âmbito da segurança da informação;
- Participar em ações de formação e sensibilização no âmbito da Cibersegurança promovidas pela ESEnfC;
- Participar qualquer evento que possa colocar em causa a segurança da informação;

No caso de desrespeito pelo disposto na presente política a **ESEnfC** promoverá os procedimentos necessários, para que o infrator responda nos termos da responsabilidade civil, criminal, contraordenacional e/ou disciplinar, que ao caso couber.

11. REVISÃO E ATUALIZAÇÃO

Todas as políticas, procedimentos e demais documentos de suporte ao **Plano de Segurança da ESEnfC**, serão revistos e atualizados sempre que existirem alterações de contexto e estratégia da **ESEnfC**, alterações da lista de partes interessadas e respetivos requisitos, ou ainda devido à realização de alterações organizativas relevantes nos seus processos decorrentes do exercício das competências atribuídas.

O Responsável de Segurança compromete-se, ainda, que esta revisão e atualização será realizada, pelo menos, anualmente.

12. PUBLICAÇÃO

Atendendo à classificação atribuída a este documento, o mesmo deverá ser divulgado com recurso a meio, preferencialmente digital acessível ao conjunto das partes interessadas constantes no **Plano de Segurança da ESEnfC**.

A sua publicação será sempre feita em modo seguro, em formato digital PDF, através do uso de controlos de segurança adequados a este objetivo.